Insert new claims 40-79 as follows:

40. (New) A device for use in an information processing system that distributes encrypted message data, the device comprising:

a receiver for receiving the encrypted message data and an enabling key block (EKB), the EKB including encrypted keys and a tag, the encrypted keys including at least one renewed key and the tag including position discrimination data that associates each of the encrypted keys with nodes and leaves of a hierarchical tree structure;

a memory for storing a key set, the key set including at least one key corresponding to a node or leaf of the hierarchical tree structure; and

A2 Cont

an encryption processor operable to (a) decrypt the encrypted keys of the received EKB using the stored key set and the position discrimination data of the received EKB to recover the at least one renewed key and (b) decrypt the received encrypted message using the at least one recovered renewed key.

41. (New) The device of claim 40, wherein the at least one renewed key is associated with a predetermined node of the hierarchical tree structure and is encrypted using a key associated with a node or leaf of the hierarchical tree structure which is subordinate to the predetermined node.

42. (New) The device of claim 40, wherein the encrypted keys of the EKB comprise only keys corresponding to a node or leaf of a simplified tree structure, the simplified tree structure being constructed from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure, and wherein the position discrimination data of the EKB indicates whether an encrypted key corresponding to a node is included in the EKB.

43. (New) The device of claim 40, wherein the encrypted keys of the EKB comprise only keys corresponding to a node or leaf of a simplified tree structure, the simplified tree structure being constructed from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure, and wherein the position discrimination data of the EKB further indicates whether an encrypted key corresponding to a predetermined node is included in the EKB and, if included, the position discrimination data indicates whether that encrypted key is at a left or right node position of the simplified tree structure which is subordinate to the predetermined node.

A2 cont.

44. (New) The device of claim 43, wherein the simplified tree structure comprises a sub-root that is a top node of an entity.

45. (New) The device of claim 40, wherein the encrypted keys of the EKB comprise only keys corresponding to a top node and a terminal node of a simplified tree structure, the simplified tree being constructed from the hierarchical tree structure by selecting only paths between the top node and the terminal node of the hierarchical tree structure, and wherein the position discrimination data of the EKB indicates whether an encrypted key corresponding to a node is included in the EKB.

46. (New) The device of claim 45, wherein the simplified tree structure is a tree having not less than three branches connecting the top node with the terminal node.

47. (New) The device of claim 40, wherein the encryption processor is operable to sequentially (a) extract the encrypted keys from the received EKB using the position discrimination data from the tag, (b) decrypt the extracted encrypted keys to obtain

the renewed key, and (c) decrypt the received encrypted message using the renewed key.

48. (New) The device of claim 40, wherein the encrypted message data represents a content key that can be used as a decryption key for decrypting encrypted content.

49. (New) The device of claim 40, wherein the encrypted message data represents an authentication key used in an authentication process.

50. (New) The device of claim 40, wherein the encrypted message data represents a key for generating an integrity check value (ICV) of content.

A3 Cont

51. (New) The device of claim 40, wherein the encrypted message data represents program code.

52. (New) A method for distributing encrypted message data, comprising:

generating an enabling key block (EKB) including a tag and encrypted keys, the encrypted keys including at least one renewed key and the tag including position discrimination data that associates each of the encrypted keys with nodes and leaves of a hierarchical tree structure; and

generating the encrypted message data using the at least one renewed key for distribution to a device.

53. (New) The method of claim 52, further comprising

decrypting the encrypted keys of the EKB using a stored key set and the position discrimination data of the EKB to recover the at least one renewed key; and

decrypting the encrypted message using the at least one recovered renewed key.

54. (New) The method of claim 53, wherein the step of decrypting the encrypted keys includes

extracting the encrypted keys from the EKB using the position discrimination data from the tag; and

decrypting the extracted encrypted keys to recover the renewed key.

55. (New) The method of claim 52, wherein the step of generating the EKB includes

A2 cont

encrypting the at least one renewed key, which is associated with a predetermined node of the hierarchical tree structure, using a key associated with a node or leaf of the hierarchical tree structure which is subordinate to the predetermined node; and

generating the position discrimination data indicating a position of the at least one renewed key in the hierarchical tree structure.

56. (New) The method of claim 52, wherein the step of generating the EKB includes

forming a simplified tree structure from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure;

generating the encrypted keys such that the encrypted keys comprise only keys corresponding to a node or leaf of the simplified tree structure; and

generating the tag such that the position discrimination data indicates whether an encrypted key corresponding to a node is included in the EKB.

57. (New) The method of claim 56, wherein the simplified tree structure comprises a sub-root that is a top node of an entity.

58. (New) The method of claim 52, wherein the step of generating the EKB includes

forming a simplified tree structure from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure;

generating the encrypted keys such that the encrypted keys comprise only keys corresponding to a top node and terminal node or leaf of the simplified tree structure; and

A2 cont.

generating the tag such that the position discrimination data indicates whether an encrypted key corresponding to a node is included in the EKB.

59. (New) The method of claim 58, wherein the simplified tree structure is a tree having not less than three branches connecting the top node with the terminal node.

60. (New) The method of claim 52, wherein the encrypted message data represents a content key that can be used as a decryption key for decrypting encrypted content.

61. (New) The method of claim 52, wherein the encrypted message data represents an authentication key used in an authentication process.

62. (New) The method of claim 52, wherein the encrypted message data represents a key for generating an integrity check value (ICV) of content.

63. (New) The method of claim 52, wherein the encrypted message data represents program code.

64. (New) A computer readable medium having a data structure readable by a computer for use in distributing encrypted message data, the medium comprising:

data fields representing an enabling key block (EKB) including a tag and encrypted keys, the encrypted keys including at least one renewed key and the tag including position discrimination data that associates each of the encrypted keys with nodes and leaves of a hierarchical tree structure; and

data fields representing the encrypted message data that was encrypted using the at least one renewed key.

65. (New) The computer readable medium according of claim 64, wherein the at least one renewed key, is associated with a predetermined node of the hierarchical tree structure and, is encrypted using a key associated with a node or leaf of the hierarchical tree structure which is subordinate to the predetermined node.

A2 cont

66. (New) The computer readable medium of claim 64, wherein the encrypted keys of the EKB comprise only keys corresponding to a node or leaf of a simplified tree structure, the simplified tree structure being constructed from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure and wherein the position discrimination data of the EKB indicates whether an encrypted key corresponding to a node is included in the EKB.

67. (New) A computer program product comprising a computer readable medium for storing computer executable instructions for use in distributing encrypted message data to a device, the device being associated with a terminal node of a hierarchical tree structure having a plurality of nodes including a top node, each node associated with a key for use in encryption, the

instructions when executed performing a process, the process comprising

forming a simplified tree structure from the hierarchical tree structure by selecting only paths between the top node and the terminal node of the hierarchical tree structure; and

generating encrypted keys such that the encrypted keys comprise only keys corresponding to a node of the simplified tree structure; and

generating a tag that includes position discrimination data which indicates whether a key corresponding to a node is included in the encrypted keys; and

forming an enabling key block (EKB) including the encrypted keys and the tag.

A3 cont.

68. (New) An information processing system, comprising:

means for receiving encrypted message data and an enabling key block (EKB), the EKB including encrypted keys and a tag, the encrypted keys including at least one renewed key and the tag including position discrimination data that associates each of the encrypted keys with nodes and leaves of a hierarchical tree structure;

means for storing a key set, the key set including at least one key corresponding to a node or leaf of the hierarchical tree structure; and

means for decrypting the encrypted keys of the received EKB using the stored key set and the position discrimination data of the received EKB to recover the at least one renewed key and for decrypting the received encrypted message using the at least one recovered renewed key.

69. (New) The information processing system according to claim 68, wherein the at least one renewed key is associated with a predetermined node of the hierarchical tree structure and is

encrypted using a key associated with a node or leaf of the hierarchical tree structure which is subordinate to the predetermined node.

70. (New) The information processing system according to claim 68, wherein the encrypted keys of the EKB comprise only keys corresponding to a node or leaf of a simplified tree structure, the simplified tree structure being constructed from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure and wherein the position discrimination data of the EKB indicates whether an encrypted key corresponding to a node is included in the EKB.

A2 cont

71. (New) The information processing system according to claim 68, wherein the encrypted keys of the EKB comprise only keys corresponding to a node or leaf of a simplified tree structure, the simplified tree structure being constructed from the hierarchical tree structure by selecting only paths between a top node and a terminal node or leaf of the hierarchical tree structure, and wherein the position discrimination data of the EKB further indicates whether an encrypted key corresponding to a predetermined node is included in the EKB and, if included, the position discrimination data indicates whether that encrypted key is at a left or right node position of the simplified tree structure which is subordinate to the predetermined node.

72. (New) The information processing system according to claim 68, wherein the decrypting means sequentially (a) extracts the encrypted keys from the received EKB using the position discriminates data from the tag, (b) decrypts the extracted encrypted keys to obtain the renewed key, and (c) decrypts the received encrypted message using the renewed key.

73. (New) An information processing method for use in decrypting encrypted message data, the method comprising:

receiving an enabling key block (EKB) including encrypted keys and a tag, the encrypted keys including at least one renewed key and the tag including position discrimination data that associates each of the encrypted keys with nodes and leaves of a hierarchical tree structure;

extracting the encrypted keys from the received EKB in accordance with the positional discrimination data from the tag; and

decrypting the extracted encrypted keys to obtain the at least one renewed key.

74. (New) The information processing method according to claim 73, wherein the decrypting step includes using a stored key set to decrypt the extracted encrypted keys, the stored key set including at least one key corresponding to a node or leaf of the hierarchical tree structure.

A3 cont.

75. (New) The information processing method according to claim 73, further comprising decrypting encrypted message data using the at least one obtained renewed key.

76. (New) The information processing method according to claim 75, wherein the encrypted message data represents a content key that can be used as a decryption key for decrypting encrypted content.

77. (New) The information processing method according to claim 75, wherein the encrypted message data represents an authentication key used in an authentication process.

A2 Cncld

78. (New) The information processing method according to claim 75, wherein the encrypted message data represents a key for generating an integrity check value (ICV) of content.

79. (New) The information processing method according to claim 75, wherein the encrypted message data represents program code.